Commission d'accès à l'information du Québec

Incidents de sécurité : mieux vaut prévenir que guérir!

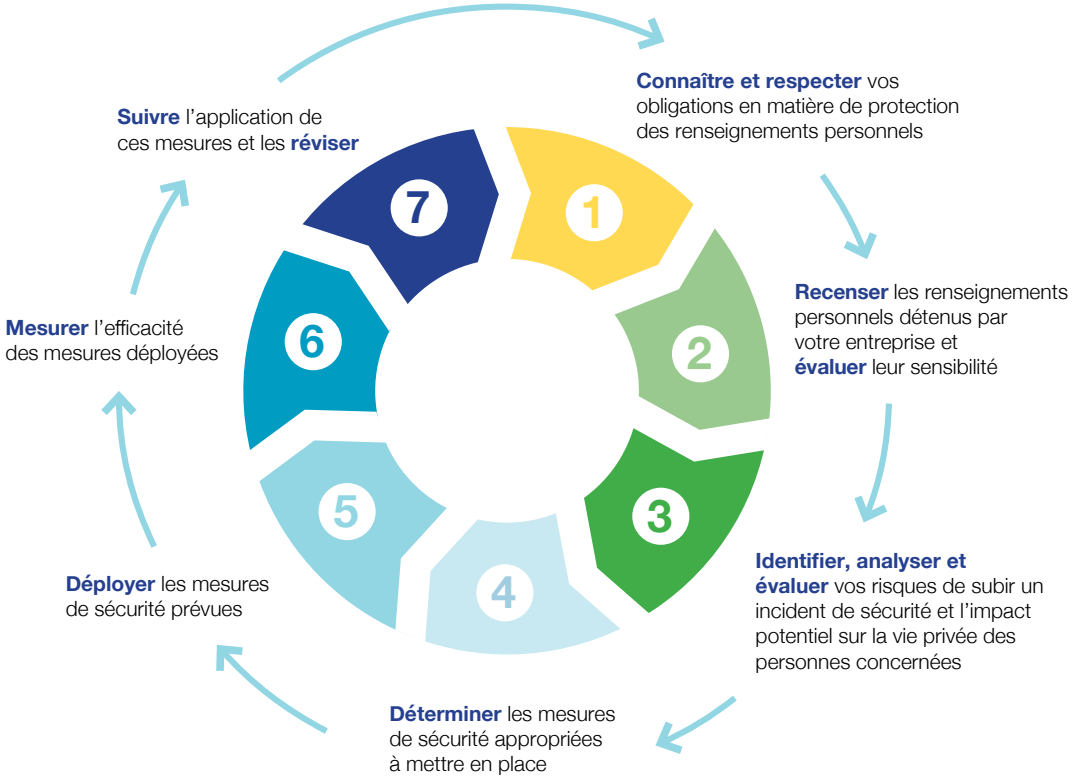
Fiche pratique
Aide-mémoire

Conseils pratiques aux entreprises

Vous pouvez limiter les risques d'un incident de sécurité impliquant des renseignements personnels au sein de votre entreprise :

- ✓ en respectant vos obligations et les principes de protection des renseignements personnels;
- ✓ en mettant en place des mesures de sécurité appropriées;
- ✓ en vous assurant de leur application et de la constance de leur efficacité.

La Commission vous propose cet **aide-mémoire** pour vous guider dans chacune des **sept étapes** de la démarche proposée dans son *guide complet* pour prévenir ou minimiser les impacts d'un incident de sécurité impliquant des renseignements personnels.



Étape 1

Connaître et respecter vos obligations

Respecter vos obligations peut vous aider à prévenir ou à minimiser les impacts d'un incident de sécurité impliquant des renseignements personnels.

Vous trouverez ci-dessous une liste de certaines obligations pouvant jouer ce rôle. D'autres obligations existent cependant. Pour en savoir davantage, consultez la page Web *Protection des renseignements personnels*.

En matière de collecte

Faites de bonnes affaires en ne collectant que les renseignements personnels nécessaires!

- ☐ Vous avez déterminé les fins de la collecte et jugé que vous aviez un intérêt sérieux et légitime pour constituer un dossier de renseignements personnels sur vos employés ou vos clients.
- ☐ Vous collectez auprès des personnes concernées uniquement les renseignements personnels nécessaires (ex. : à leur embauche et à la gestion de leur dossier d'employé ou pour offrir votre bien ou votre service).

> **Rappelez-vous :** un pirate ne peut voler les renseignements personnels que votre entreprise n'a pas collectés!

- ☐ Votre collecte se fait auprès de la personne concernée par des moyens licites (c'est-à-dire légaux et légitimes).
- ☐ Avant de constituer un dossier sur vos employés ou vos clients, vous les avez informés :
  - ☐ des finalités du dossier;
  - ☐ de l'utilisation qui sera faite de leurs renseignements personnels;
  - ☐ des catégories de personnes qui y auront accès au sein de votre entreprise;
  - ☐ de l'endroit où les renseignements seront détenus.
- ☐ Vous avez obtenu le consentement des personnes concernées avant de collecter leurs renseignements personnels auprès d'un tiers, à moins d'une exception prévue par la *Loi sur le privé*.

  Ce consentement est manifeste, libre, éclairé et donné à des fins spécifiques. De plus, il ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles vous l'avez demandé.

> **Rappelez-vous :** une personne informée de ses droits en vaut deux! Elle sera beaucoup plus attentive à la protection de ses renseignements personnels et alerte en cas d'incident si elle sait par exemple quelles catégories de personnes ou tiers sont susceptibles de les utiliser ou de les détenir.

- ☐ Vous avez mis en place des mesures de sécurité appropriées propres à assurer la protection des renseignements personnels collectés.

  Ces mesures sont raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.
- ☐ Vous avez prévu une révision périodique des différentes collectes de renseignements personnels concernant vos employés et vos clients.

Pour aller plus loin, consultez :

- ☐ La page Web *La collecte de renseignements personnels*
- ☐ La fiche *Pièces d'identité : entreprises*

En matière d'utilisation

C'est élémentaire : il ne faut utiliser que les renseignements personnels nécessaires !

- ☐ Vous donnez accès aux renseignements personnels uniquement aux personnes ayant la qualité pour recevoir cet accès au sein de l'entreprise, lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions.

> **Rappelez-vous** qu'un employé détenant des droits d'accès restreints ne peut compromettre l'ensemble des renseignements détenus par votre entreprise !

- ☐ Une fois l'objet du dossier accompli, vous limitez l'utilisation de renseignements personnels à celle à laquelle consent la personne concernée, sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement du gouvernement.
- ☐ Vous avez mis en place des mesures de sécurité appropriées propres à assurer la protection des renseignements personnels utilisés.

  Ces mesures sont raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.

En matière de communication

Ne communiquez que ce qui est autorisé et de manière sécurisée !

- ☐ Vous avez obtenu le consentement des personnes concernées pour communiquer leurs renseignements à un tiers (ex. : assureur ou prestataire de services), à moins d'une exception prévue par la Loi sur le privé.
- ☐ Vous avez mis en place des mesures de sécurité appropriées propres à assurer la protection des renseignements personnels communiqués.

  Ces mesures sont raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.
- ☐ Vous et votre personnel veillez à ce que la personne à qui vous communiquez ou confiez des renseignements personnels, à l'extérieur de la province, assure un niveau de protection équivalent à celui que vous êtes tenus de respecter.

En matière de conservation

Ne conservez que des renseignements exacts et à jour et de manière sécurisée !

- ☐ Les renseignements personnels que vous détenez sur vos employés ou vos clients sont exacts et à jour au moment où vous les utilisez pour prendre une décision à leur sujet.
- ☐ Vous avez mis en place des mesures de sécurité appropriées propres à assurer la protection des renseignements personnels conservés.

  Ces mesures sont raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.

En matière de destruction

Les renseignements dont la finalité est accomplie doivent être détruits !

- ☐ Vous détruisez les documents contenant des renseignements personnels de manière sécuritaire dès que la finalité pour laquelle ils ont été collectés est accomplie, sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement du gouvernement (ex. pour des obligations fiscales).

> **Rappelez-vous :** un pirate ne peut voler les renseignements personnels que votre entreprise a détruits !

Pour aller plus loin, consultez :

- ☐ La fiche *Destruction des documents contenant des renseignements personnels*

Étape 2

Recenser les renseignements personnels détenus par votre entreprise et évaluer leur sensibilité

Comprendre les renseignements que vous détenez vous permettra de mieux les protéger !

- ☐ Vous avez réalisé un inventaire des renseignements personnels que votre entreprise détient. Cet inventaire contient :
  - ☐ Les types de renseignements personnels que votre entreprise collecte sur ses clients ou ses employés (ex. : nº de carte de crédit, adresse, nº de téléphone);
  - ☐ Les fins (objectifs recherchés, résultats attendus) pour lesquelles il est nécessaire que votre entreprise collecte ces renseignements personnels;
  - ☐ Le degré de sensibilité des renseignements personnels collectés;
  - ☐ La façon dont ces renseignements sont recueillis par votre entreprise (comment);
  - ☐ Les catégories de personnes autorisées à y avoir accès au sein de l'entreprise ou à l'extérieur (tiers);
  - ☐ Le contexte dans lequel ces renseignements sont utilisés ou communiqués au sein (ou à l'extérieur) de l'entreprise, ou la façon dont ils le sont;
  - ☐ L'endroit où sont conservés ces renseignements, sur quel(s) support(s) et dans quelles conditions;
  - ☐ La façon dont l'entreprise dispose de ces renseignements une fois que la finalité justifiant leur collecte est atteinte.

Étape 3

Identifier, analyser et évaluer les risques

Ne pas évaluer ses risques est un risque encore plus grand !

- ☐ Vous avez identifié les situations ou les évènements (risques) pouvant raisonnablement survenir et menacer la sécurité des renseignements personnels que votre entreprise détient (ex. : vol, collecte excessive ou divulgation non autorisée de renseignements personnels).
- ☐ Vous avez analysé les causes susceptibles de générer ces risques (ex. : mécanismes de surveillance insuffisants ou inexistants, manque de connaissances ou de formation, erreurs dans la manipulation des renseignements).
- ☐ Vous avez évalué l'impact potentiel de chacun des risques (ex. : très faible et / ou inexistant; faible; grand; très grand, etc.).
- ☐ Vous avez estimé les probabilités que ces risques se matérialisent.
- ☐ Vous avez considéré les stratégies et mesures de sécurité existantes.
- ☐ Vous avez déterminé le seuil de tolérance acceptable pour chaque risque.

Étape 4

Déterminer les mesures de sécurité appropriées

Adopter des mesures de sécurité appropriées : un premier pas vers des renseignements protégés!

- ☐ Par ses actions, la haute direction démontre que la protection des renseignements personnels est une priorité organisationnelle. En cela, elle fait montre d'un leadership fort et mobilisant :
  - ☐ en approuvant les mesures de sécurité mises en place et en assurant leur contrôle;
  - ☐ en faisant leur promotion active auprès du personnel;
  - ☐ en fournissant les ressources nécessaires pour assurer l'implantation et le maintien d'une culture forte de protection des renseignements personnels au sein de l'entreprise.
- ☐ Vous avez désigné une personne responsable de la protection des renseignements personnels au sein de votre entreprise.
- ☐ Votre entreprise a adopté des mesures efficaces de gouvernance et de gestion des renseignements personnels qu'elle détient. Par exemple :
  - ☐ Votre entreprise offre régulièrement à son personnel des séances de formation et de sensibilisation sur la protection des renseignements personnels et sur les politiques et directives en vigueur.
  - ☐ Votre entreprise a adopté une politique, des directives ou des procédures sur l'utilisation d'appareils informatiques mobiles à l'extérieur du lieu de travail.
  - ☐ Dans le cas de contrats avec des tiers comme des prestataires ou des fournisseurs de services, votre entreprise a adopté des politiques, procédures ou directives établissant les exigences en matière de protection des renseignements personnels.
- ☐ Votre entreprise a adopté des mesures de sécurité techniques visant la protection des renseignements personnels qu'elle détient. Par exemple :
  - ☐ Votre entreprise dispose de politiques, de directives ou de procédures pour orienter son personnel relativement aux mesures à appliquer pour sécuriser ses réseaux (y compris sans fil), prévenir les attaques contre les logiciels malveillants, gérer les accès et les privilèges des utilisateurs, etc.
- ☐ Votre entreprise a adopté des politiques, des directives ou des procédures concernant les mesures de sécurité physique à appliquer pour assurer la protection des renseignements personnels qu'elle détient (ex. : local et classeur fermés à clef, accès limités et autres).
- ☐ Votre entreprise a adopté d'autres politiques, procédures ou directives que celles énoncées précédemment qui peuvent avoir un impact positif sur la prévention des incidents de sécurité impliquant des renseignements personnels.

Étape 5

Déployer les mesures de sécurité appropriées

Prévoyez le déploiement de vos mesures et assurez-en une mise en œuvre complète et intégrée!

- ☐ Vous avez élaboré un plan d'action en concertation avec les personnes qui auront la responsabilité de le mettre en œuvre.
- ☐ Vous avez élaboré une stratégie de communication afin de faire connaître vos mesures à l'ensemble de votre personnel.
- ☐ Les mesures mises en place sont claires, complètes, concrètes et cohérentes.

Étape 6

Mesurer l'efficacité des mesures déployées

Prenez la mesure de vos mesures !

- ☐ Vous avez mesuré la performance des stratégies et des moyens de sécurité que vous avez mis en place par le biais d'outils de mesure (ex. : exercice d'hameçonnage auprès du personnel avant et après une campagne de sensibilisation sur le sujet) ou d'autres sources de rétroaction (ex. : analyse des plaintes reçues par la clientèle au regard des pratiques de l'entreprise en matière de protection des renseignements personnels).
- ☐ Vous avez réévalué le niveau de chacun des risques à la lumière des mesures déployées.

Étape 7

Surveiller l'application de ces mesures et les réviser

Protéger les renseignements personnels n'est pas l'affaire d'une seule journée !

- ☐ Vous avez mis en place des mécanismes pour surveiller de manière active l'efficacité des mesures de sécurité déployées.
- ☐ Vous réévaluez régulièrement l'efficacité de ces mesures et les mettez à jour.
- ☐ Votre entreprise a adopté une politique, des directives ou des procédures sur la gestion des incidents de sécurité pouvant porter atteinte à la protection des renseignements personnels (ex. : procédures pour détecter, consigner ou rapporter les incidents et y répondre, incluant les mesures de mitigation des risques associés à de tels incidents, et stratégies de prévention pour éviter qu'ils se reproduisent).

Des questions ?

Pour joindre la Commission :

TÉLÉPHONE SANS FRAIS
1 888 528-7741

COURRIEL
cai.communications@cai.gouv.qc.ca

SITE INTERNET
www.cai.gouv.qc.ca